REMARKS

Reconsideration of the present application in view of the enclosed amendments and remarks is respectfully requested.

Claims 1-80 have been canceled. Claims 81-124 have been added. Claims 81, 98, and 111 are the pending independent claims.

ARGUMENT

The Office Action includes claim rejections based on statutory double patenting under 35 U.S.C. § 101 and based on 35 U.S.C. § 103(a).

Statutory Double Patenting

The Office Action rejects claims 1-80 based on statutory double patenting under 35 U.S.C. § 101, in light of claims 1-80 of U.S. patent application no. 09/539,344, which is the parent of the present application. To the extent those rejections might be applied to the claims as amended, Applicants respectfully traverse those rejections.

35 U.S.C. § 103(a)

The Office Action rejects claims 1-80 under 35 U.S.C. § 103(a) as being unpatentable over U.S. patent no. 5,809,546 to Paul Gregory Greenstein et al. (hereinafter "Greenstein") in view of U.S. patent no. 4,419,724 to Michael H. Branigin et al. (hereinafter "Branigin"). To the extent those rejections might be applied to the pending claims, Applicants respectfully traverse.

The present invention pertains to firmware or other software that facilitates enhanced security and/or integrity for processing systems, and to related systems, methods, and apparatuses. For instance, claim 111 involves system with hardware features including a processor and memory, as well as software features including a "processor executive" that executes on a processor. In particular, according to claim 111, the processor executive runs an operating mode of the processor known as

"isolated execution mode." In addition, one of the operations performed by the processor executive is to launch an operating system (OS) executive.

By contrast, Greenstein pertains to a method for managing input/output (I/O) buffers in shared storage. The Office Action asserts that the central processing unit (CPU) illustrated at reference number 101 in Fig. 1 of Greenstein constitutes a "processor executive." In the context of the present application, the assertion that a CPU is the same thing as a processor executive is fundamentally incorrect.

In the present application, claim 111 pertains to a platform comprising memory and a processor. In addition to those hardware components, the platform comprises software – specifically, "instructions" that cause the hardware to perform certain operations when the instructions are "executed in the platform." In particular, claim 111 recites a "processor executive" that executes on the platform's processor. Thus, in the context of the precent application, the term "processor executive" clearly denotes software to execute on a processor. In addition, claim 114 pertains to an operation in which the "processor executive" is loaded into memory (specifically, a portion of memory known as an "isolated memory area"). Claim 114 therefore further supports the inescapable conclusion that a processor executive is not the same thing as a CPU.

For the above and other reasons, Applicants respectfully traverse the assertion in the Office Action that a processor executive "is met by" CPU 101 in Fig. 1 of Greenstein.

The Office Action also seems to misinterpret the term "operating system executive" (or "OS executive"). In the context of the present application, an OS executive is a type of software – specifically, software that relates to an operating system). Of course, the term "operating system" is well known in the art to cover software products such as MICROSOFT WINDOWS, LINUX, etc.

Branigin pertains to a main bus interface package. Like Greenstein, Branigin does not disclose or suggest a processor executive that executes on a processor and launches an OS executive. Consequently, even if Greenstein and Branigin were to be combined, the combination would not render claim 111 obvious. Further, claims 81 and 98 also relate to a processor executive that executes on a processor

and launches an OS executive, and all other pending claims depend ultimately from claim 81, claim 98, or claim 111. The cited art therefore does not render any of the pending claims unpatentable.

In addition, the pending claims recite numerous additional features that are not disclosed or suggested by either Greenstien or Branigin. For example, claim 111 recites a "processor is capable of running in an isolated execution mode within a ring 0 operating mode, wherein the processor supports one or more higher ring operating modes, and wherein the processor supports a non-isolated execution mode within at least the ring 0 operating mode." Neither Greenstien nor Branigin discloses or suggests a processor that supports normal and isolated execution modes within a ring 0 operating mode.

Claim 111 also recites operations of (a) loading the OS executive "into the isolated memory area," (b) "verifying the OS executive, using the processor executive," and (c) launching the OS executive "after verifying the OS executive." Neither Greenstien nor Branigin discloses or suggests any of those operations.

Numerous additional features from the pending claims that are not disclosed or suggested by Greenstein and Branigin could also be noted. For instance, claim 112 recites that the OS executive is verified "during a process of booting the platform." Claim 115 recites "launching the OS executive to run in the isolated execution mode." Claim 117 recites that the system includes a "platform key" (PK), and "the platform verifies the OS executive, based at least in part on the PK."

Further, claim 124 involves a non-interruptible atomic sequence of operations such as (a) "reading a thread count register in a chipset to determine if the processor is the first processor in the isolated execution mode;" (b) "configuring the processor in the isolated execution mode;" (c) "loading a processor executive handler into the isolated memory area;" and (d) "transferring control to the loaded processor executive handler." None of those features is disclosed or suggested by Greenstien or Branigin.

For these and other reasons, all pending claims are allowable.

INFORMATION DISCLOSURE STATEMENTS

Applicants also request confirmation that the Examiner has considered the references listed on the information disclosure statements (IDSs) and eIDSs filed on the following dates: (a) IDS – September 4, 2001, (b) IDS – April 5, 2002, (c) IDS – December 17, 2003, (d) IDS – June 29, 2004, and (e) eIDS – June 29, 2004. Copies of those IDSs and eIDS are enclosed for reference. Confirmation of consideration is requested for the following reasons: The Office Action did not include page two of the IDS that was filed on September 4, 2001. The Office Action did not include page two of the IDS that was filed on April 5, 2002. The Office Action did not include initials for the two "Foreign Patent Documents" listed on the IDS that was filed on December 17, 2003. The Office Action did not include a copy of the IDS that was filed on June 29, 2004. The Office Action did not include a copy of the eIDS that was filed on June 29, 2004.

CONCLUSION

For reasons including those set forth above, claims 81-124 are all in condition for allowance.

As indicated above, Applicants also request confirmation that all references cited by Applicants have been considered.

If the Examiner has any questions, the Examiner is invited to contact the undersigned at (512) 732-3927. Early issuance of Notice of Allowance is respectfully requested.

Respectfully submitted,

Dated: 8/27/04

Michael R. Barré
Patent Attorney
Intel Americas, Inc.
Registration No. 44,023
(512) 732-3927

c/o Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

8-30-2004

Gayle Bekish

Name of Person Mailing Correspondence

Signature

8-30-2004

Date